

## **REMARKS**

### **Status**

This Amendment is responsive to the Office Action dated April 21, 2005, in which claims 1-43 were rejected. Claims 1-43 are pending in the application, and are presented for reconsideration and allowance.

### **Claim Rejection - 35 USC 102**

Claims 1-3, 7-9, 11-13, 15-18, 30-34, and 37-39 stand rejected under 35 USC 102 as being anticipated by US Patent Application Publication No. 2002/0083323 (Cromer). This rejection is respectfully traversed.

The present invention relates generally to the processing and authenticating of a digitally captured image while providing flexibility and portability of the image capture device used to capture the image. More specifically, the present invention provides a system and method of verifying the authenticity of a digital image on the basis of an authentication signature not stored in the digital image capture device but rather at a secure remote location. The digital image is not encrypted nor stored at the remote location. As such, the utility of the digital image is not reduced. Rather, the authentication signature is accessed each time the authenticity of the digital image is at issue. If the digital image maintains the same signature, the digital image is considered to be authentic.

According to the invention defined by claim 1, there is provided a method for processing for later authentication a digital still image captured using a digital image capture device. The method includes the steps of transmitting signature data from a remote location to the digital capture device, associating an image identification with the captured digital still image, applying the signature data to the captured digital still image to produce an authentication signature representative of the captured digital still image, associating the authentication signature with the image identification, transmitting the authentication signature to the remote location, and storing the signature data, the authentication signature, and the image identification at the remote location.

The invention has several advantages: (1) Since the digital image need not be encoded, marked or encrypted, the captured digital image can be

provided in a memory card or in an internet database for viewing on a home computer; (2) Since the remote location need not store image information, but only authentication and signature information, the size, cost, and complexity of the remote location is reduced; (3) Since the digital image remains in the possession of the user, the user controls the image so that it can be used for viewing and verification need only be established as needed; and (4) Since only a small amount of data is sent to the remote location, communication channels with lower bandwidth, such as cellular telephony, can be used to transfer the data that will be used later for verification.

Contrary to the assertion set forth in the Office Action, Cromer clearly does not anticipate under 35 USC 102 the present invention as defined by the rejected claims. Cromer discloses a method and system for enabling an image to be authenticated. The digital capture of the image, the generation of the authentication data, the storage of the image and of the authentication data, and the verification of the authenticity of the captured digital image all take place within the same digital capture device. Contrary to the Office Action's statements, there is no disclosure in Cromer of communicating with a remote location. The following steps of method of claim 1 are clearly not disclosed in Cromer. The paragraphs referred to in Cromer by the Office Action clearly do not support the teaching of the following omissions.

1) Transmitting signature data from a remote location to the digital image capture device. In Cromer, "the image file and the digital signature of the camera are stored in memory in the camera" [0021]. "The captured image and the digital signature of the camera are stored in a file within the memory of the camera" [0023]. Moreover, the claimed invention does not use the digital signature of the camera in the authentication process. The claimed invention is advantageous over the Cromer technique because Cromer uses only the digital signature of the camera in its authentication process, while the claimed invention can use different signature data received from the remote location for different digital images. One purpose of the Cromer process is to authenticate that a particular image was taken with a specific camera.

2) Applying the signature data to the captured digital still image to produce an authentication signature representative of the captured digital still

image. The latter step is the hashing step. In the claimed invention, the signature data is used on the digital image to create a unique signature for the image. In Cromer, the digital signature is merely associated with the digital image and then hashed by the algorithm resident in the camera together with the digital image to create a digest. Whereas Cromer employs an unmodified hashing algorithm to act upon the combination of image data and digital signature, the claimed invention uses a hashing algorithm modified by signature data to hash the image.

3) Transmitting the authentication signature to the remote location. In Cromer, the authentication data is never transmitted outside of the camera.

4) Storing the signature data, authentication signature, and image identification at the remote location. There is no disclosure in Cromer of storing any authentication data at a remote location.

5) The claimed invention does not use the Cromer process of encryption of the digest via a photographer's private key to create a digital signature for the photographer.

With respect to independent claim 8, the above arguments with respect to claim 1 are also applicable. In addition, the additional steps recited in claim 8 are not disclosed in Cromer since Cromer only performs authentication in the digital camera and does not disclose performing any authentication steps at a remote location. Accordingly, claim 8 is clearly not anticipated by Cromer.

With respect to independent claim 12, the above arguments with respect to Claim 1 are equally applicable. Moreover, there is no disclosure in Cromer of the additional steps of claim 12 since authentication in Cromer takes place in the camera and not in association with a remote location. The Office Action's assertion that in Cromer there is communication with a remote location, such as the Sport's Illustrated system, is unsupported in Cromer. Cromer's paragraphs [0026] and [0019] read as follows:

"[0026] Furthermore, the smart card/RF interface could also contain the public key and certificate of the owner or intended owners of photographs. For example, a photographer for Sports Illustrated could have Sports

Illustrated's public key and certificate associated with the camera that she is using.”

“[0019] The mechanism employed by the present invention preferably comprises a Radio Frequency (RF) interface or a smart card which is coupled to the digital camera ...“

These passages from Cromer mention no Sports Illustrated system containing authentication information with which the camera is in communication with. Rather, the smart card or RF interface is coupled to the digital camera and contains the encryption information. The RF interface is probably an RFID system containing the encryption information. There is no mention of encryption in the method of claim 12 so the teaching of Cromer is inapplicable to anticipate claim 12.

With respect to independent claims 16 and 30, the same arguments above relating to the inapplicability of Cromer are applicable to the patentability of claims 16 and 30 over Cromer. Since there is no disclosure in Cromer of any communication with a remote location relating to authentication of digitally captured images and since the invention defined by claims 16 and 30 do not use the digital signature of the camera, the digital signature of the photographer, and the encryption disclosed in Cromer for digital image authentication, claims 16 and 30 clearly are not anticipated by Cromer.

With respect to the claims dependent from independent claims 1, 8, 12, 16, and 30, rejected as being anticipated by Cromer, the same arguments given above relating to the patentability of these claims over Cromer are applicable to the dependent claims.

Clearly the claims rejected under 35 USC 102 are novel, and therefore allowable over Cromer and the other cited art.

### **Claim Rejection - 35 USC 103**

Claim 4 stands rejected under 35 USC 103 as being unpatentable over US Patent Application Publication No. 2002/0083323 (Cromer). Claims 10 and 14 stand rejected under 35 USC 103 as being unpatentable over Cromer in view of Schneier (Applied Cryptography, 1996, John Wiley and Sons, Inc., Page 56). Claims 5, 19, 21-25, 27-29, 35-36, and 42-43, stand rejected under 35 USC

103 as being unpatentable over Cromer in view of US Patent Application Publication 2002/0023220 (Kaplan). Claims 6, 20, and 26 stand rejected under 35 USC 103 as being unpatentable over Cromer in view of US Patent Publication No. 2001/000712 (Lambert). Claims 40 and 41 stand rejected under 35 USC 103 as being unpatentable over Cromer in view of US Patent No. 5,499,294 (Friedman). These rejections are respectfully traversed.

With respect to the claims rejected under 35 USC 103 as being unpatentable over Cromer alone or in combination with either Schneier, Kaplan, Lambert, or Friedman, the arguments for patentability over Cromer given above are equally applicable to these rejections. In addition, the latter four references are inapplicable to the claimed inventions because each discloses either encoding or encrypting the data processed. As discussed above, the present invention need not include encoding or encryption. The rejected claims are therefore nonobvious over the cited references and should be allowed.

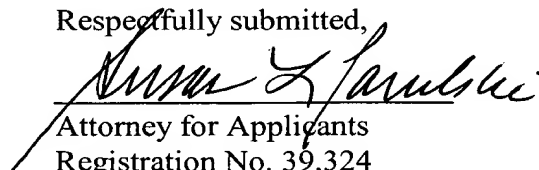
#### **Summary**

Should the Examiner consider that additional amendments are necessary to place the application in condition for allowance, the favor is requested of a telephone call to the undersigned counsel for the purpose of discussing such amendments.

For the reasons set forth above, it is believed that the application is in condition for allowance. Accordingly, reconsideration and favorable action are respectfully solicited.

The Commissioner is hereby authorized to charge any fees in connection with this communication to Eastman Kodak Company Deposit Account No. 05-0225.

Respectfully submitted,

  
Attorney for Applicants  
Registration No. 39,324

Susan L. Parulski/law  
Rochester, NY 14650-2201  
Telephone: (585) 477-4027  
Facsimile: (585) 477-4646